Business Case Models

Description

Presents a conceptual framework for quantifying cost and benefits of investments in secure coding techniques. Guidance for implementing the framework will include the variables and data elements to focus on and means to measure and quantify them. With these measurements, one can calculate the economic benefits (cost) of these investments. Details are also provided on current practices and current research on the case for secure coding techniques.

Overview Articles

Name	Version Creation Time	Abstract
Making the Business Case for Software Assurance	11/2/09 2:02:02 PM	It is essential to be able to make a cost/benefit argument in order to justify investment in software assurance during the software development process. Although we are making some strides in identifying costs, quantifying the benefits can be much more elusive. In this article we give an overview of the Business Case content area.

Most Recently Updated Articles [Ordered by Last Modified Date]

Name	Version Creation Time	Abstract
Making the Business Case for Software Assurance	11/2/09 2:02:02 PM	It is essential to be able to make a cost/benefit argument in order to justify investment in software assurance during the software development process. Although we are making some strides in identifying costs, quantifying the benefits can be much more elusive. In this article we give an overview of the Business Case content area.
It’s a Nice Idea but How Do We Get Anyone to Practice It? A Staged Model for Increasing Organizational Capability in Software Assurance	3/3/09 5:29:33 PM	This article presents a standard approach to increasing the security capability of a typical IT function. This five level model involves the development of a common set of security best practices, which are then deployed in a staged fashion to leverage an optimal security capability across the organization. At the lowest level the organization will have minimal assurance of security

		capability. At the highest level the organization can be trusted to produce products and provide services that are both dependable and secure. The article presents the practices and the maturity framework. It also discusses the practical mechanisms for implementing this model in a real world setting.
Models for Assessing the Cost and Value of Software Assurance	2/25/09 3:41:12 PM	It is not enough to simply estimate the cost of doing secure software assurance: you must also justify it from a value perspective. This paper presents IT valuation models that represent the most commonly accepted approaches to the valuation of IT and IT processes. These models can be categorized into four initial types: investment based, cost based, environmental/contextual, and quantitative estimation. However, the general conclusion is that there are only two valid ways to approach valuation of the secure software assurance process: quantitative and environmental.
What Measures Do Vendors Use for Software Assurance?	2/10/09 3:54:40 PM	Books and articles frequently exhort developers to build secure software by designing security in. A few large companies (most notably Microsoft) have completely reengineered their development process to include a focus on security. However, for all except the largest vendors, software security (or software assurance) is a relatively recent phenomenon, and one with an uncertain payoff. In this article, we examine what vendors do to ensure that their products are reasonably secure. Our conclusion is that software vendors put significant energy into software security, but there is significant variation in where they invest their money.
Estimating Benefits from Investing in Secure Software Development	11/14/08 4:00:03 PM	This article discusses the costs and benefits of incorporating security in software development and

		presents formulas for calculating security costs and security benefits.

All Articles [Ordered by Title]

Name	Version Creation Time	Abstract
A Common Sense Way to Make the Business Case for Software Assurance	11/14/08 3:57:42 PM	This article demonstrates how a true cost/benefit for secure software can be derived using three generic practice areas: (1) threat/risk understanding, (2) implementation of security requirements, and (3) operational security testing. Having an accurate cost for these aspects of the software assurance process would allow decision makers to make intelligent decisions about the level of investment they wish to make.
Business Considerations and Foundations for Assuring Software Security: Business Case Models for Rational Action	11/14/08 3:58:27 PM	In this article, we discuss business considerations and business case models for assuring software security. Specifically, we review industry forces and enterprise considerations that feed into business case models.
Calculating Security Return on Investment	11/14/08 3:59:14 PM	With the dramatic increase in cyberspace incidents and perceptions about the high cost of security readiness and survivability, there is a need for a method to reason about and compute security return on investment (ROI). This article describes several such methods.
Estimating Benefits from Investing in Secure Software Development	11/14/08 4:00:03 PM	This article discusses the costs and benefits of incorporating security in software development and presents formulas for calculating security costs and security benefits.
It’s a Nice Idea but How Do We Get Anyone to Practice It? A Staged Model for Increasing Organizational Capability in Software Assurance	3/3/09 5:29:33 PM	This article presents a standard approach to increasing the security capability of a typical IT function. This five level model involves the development of a common set of security best practices, which are then deployed in a staged fashion to leverage an

		optimal security capability across the organization. At the lowest level the organization will have minimal assurance of security capability. At the highest level the organization can be trusted to produce products and provide services that are both dependable and secure. The article presents the practices and the maturity framework. It also discusses the practical mechanisms for implementing this model in a real world setting.
Making the Business Case for Software Assurance	11/2/09 2:02:02 PM	It is essential to be able to make a cost/benefit argument in order to justify investment in software assurance during the software development process. Although we are making some strides in identifying costs, quantifying the benefits can be much more elusive. In this article we give an overview of the Business Case content area.
Maturity Framework for Assuring Resiliency Under Stress	8/28/08 2:43:20 PM	Managing assurance is to reason about the emergent properties of large complex software-intensive systems; to take action to steer enterprise commitment towards their assurance; and to guide buyers, users, and the public in setting their level of confidence in these systems and systems of systems. The purpose of this article is to specify a framework for assuring the resiliency of the critical infrastructure through a management, process, and engineering framework of capabilities and solutions along with the model-based business, technical, and operational claims, arguments, and evidence useful in its assessment.
Models for Assessing the Cost and Value of Software Assurance	2/25/09 3:41:12 PM	It is not enough to simply estimate the cost of doing secure software assurance: you must also justify it from a value perspective. This paper presents IT valuation models that represent the most commonly accepted approaches

		to the valuation of IT and IT processes. These models can be categorized into four initial types: investment based, cost based, environmental/contextual, and quantitative estimation. However, the general conclusion is that there are only two valid ways to approach valuation of the secure software assurance process: quantitative and environmental.
What Measures Do Vendors Use for Software Assurance?	2/10/09 3:54:40 PM	Books and articles frequently exhort developers to build secure software by designing security in. A few large companies (most notably Microsoft) have completely reengineered their development process to include a focus on security. However, for all except the largest vendors, software security (or software assurance) is a relatively recent phenomenon, and one with an uncertain payoff. In this article, we examine what vendors do to ensure that their products are reasonably secure. Our conclusion is that software vendors put significant energy into software security, but there is significant variation in where they invest their money.

Related Articles

The article Making Security Governance Investment Decisions – A Dashboard Approach[1], in the Governance & Management content area, presents an approach for selecting security governance investments using business-based criteria. The approach and supporting tool define seven decision criteria categories, each supported by three or more indicators. Categories and indicators are ranked and applied to a series of investments. Individual investment scores are presented for discussion and evaluation by decision makers. While security governance is the current focus, this approach can be applied to any class of security investments, including software assurance.

Making the Business Case for Software Assurance[2] provides guidance for those who want to make the business case for building software assurance into software products during each software development life-cycle activity. The business case defends the value of making additional efforts to ensure that software has minimal security risks when it is released and shows that those efforts are most cost-effective when they are made appropriately *throughout* the development life cycle.

[1] http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management/985-BSI.html (Making Business-Based Security Investment Decisions – A Dashboard Approach)

[2] http://www.sei.cmu.edu/library/abstracts/reports/09sr001.cfm